WEDI SNIP – Transactions Work Group
Testing Sub Work-Group

Transaction Compliance and Certification

A White Paper Describing the Recommended Solutions For Compliance Testing and Certification of the HIPAA transactions

Version 3.0

08/26/02

The following draft document has been prepared by WEDI SNIP (Strategic National Implementation Process) for the express purpose of soliciting industry review and input. All comments received by or before the comment closing date will be considered for inclusion in the associated final document.

WEDI SNIP recognizes the critical importance of Industry review and input to the successful implementation of HIPAA. So please take this opportunity to participate and let your voice be heard.

Please visit the WEDI SNIP website at snip.wedi.org to obtain current copies of all white papers. If you are interested in additional information about WEDI SNIP or for membership information, you can contact us at:

Strategic National Implementation Process
12020 Sunrise Valley Dr., Suite 100
Reston,VA. 20191
703-391-2714

Purpose and Scope

Purpose

The WEDI SNIP Transaction Set Testing Sub Workgroup has identified issues related to the testing and compliance certification of transactions as related to the HIPAA Transaction and Code Sets Final Rule. The purpose of this white paper is to:

1. Document the different types of testing available to the health care industry.
2. Identify the benefits of testing standards for compliance and certification of said data.
3. Document the savings that can be realized from testing and compliance certification.
4. Document our suggestions for compliance certification provided by the certification tools/services.

Scope

The scope of this white paper will address the following specific testing and certification issues:

1. What are the differences between transaction compliance testing and certification?
2. What are the different types of testing suggested for HIPAA transaction compliance?
3. What types of transaction testing are recommended before starting "business-to-business" testing between providers and payers. In addition, what types of testing do we recommend as sufficient for an entity's approval processes?
4. What other issues, related to transaction testing, should be considered for successful compliance testing, certification and payer acceptance?
5. What entities provide compliance testing facilities today? What types of transaction testing do they provide?
6. Who will certify the certification systems?
7. What do we recommend in selecting a compliance testing system or service?

Note: In the past, this white paper had referred to the different types of testing as levels. However, the word "level" gave the incorrect impression that these types of testing built on each other in some manner and that the testing could be stopped at a certain level. In order to try to correct this misperception, we are now calling them "types" of testing in order to more clearly convey the notion that they are independent of each other. We recommend that all of these types of testing be completed for HIPAA compliance.

Definition of Terms:

The following terms are defined as follows for use in the text of this white paper:

Certification: The independent assessment of HIPAA compliance via a third-party tool. For example, if you are using a translator for your internal testing, you can achieve certification by verifying and validating your transactions with a certification tool/service listed in the Vendor Listing on the WEDI SNIP website. The Vendor Listing can be found on the WEDI SNIP website at http://snip.wedi.org. The types/levels of certification of HIPAA compliance necessary are dictated by the needs of an enterprise. Certification is not a 100% guarantee that all covered entities will be able to accept and process your transactions.

Testing: The term testing is used in two separate manners in this white paper. One manner refers to the internal processes of developing and validating your transactions prior to trading files with any trading partner. The other is the process of exchanging files with your trading partner after the internal process has been completed. The verbiage of the paper will clarify the intent of the term "testing" as it is used in the context of the paragraph in which it is contained.

Overview

With the passing of HIPAA and its Administrative Simplification Compliance Act (ASCA), the health care industry has had to take a step back and re-assess their processing systems and business functions in order to accommodate the mandated regulations set forth by HIPAA. In order to adopt new standards in receiving and exchanging electronic health information, many trading partners have had to make extensive changes to their processing and/or management systems in a relatively short timeframe.

While there is an additional one-year grace period that can be realized if a trading partner were to file for a compliance extension, huge amounts of testing may occur within the allotted six-month time period (April – October 2003). This could potentially overwhelm both health plans and providers in their HIPAA endeavors. The majority of changes may affect data that is generated for exchange. These new changes and data must be tested extensively to maintain the integrity and effectiveness of business processing and of the driving transactions to ensure the data content with respect to internal application systems is still intact. This in-depth testing should first occur internally to gain a level of confidence in being able to accept, process, and generate a compliant transaction before integrating outside trading partners.

The current practice of testing all aspects of transaction compliance among trading partners leads to redundantly testing the same basic EDI functionality between all trading partners. Either because a trading partner is not interested in certain aspects of the transactions or is especially interested in other aspects, subsequent trading partners do not normally accept previous successful testing results from another trading partner. Under HIPAA, given that the Implementation Guides (IGs) specify certain well-defined functionality, if each trading partner candidate independently tests against the IG defined functionality, the testing among trading partners could be greatly reduced. In fact, without this reduction of the duplicative testing of the basic HIPAA functionality, it may be unreasonable to expect the industry to complete testing of the HIPAA transactions within the mandated timeframe.

Different from past EDI experiences, the HIPAA requirements are not only to move to a standard format, but also to data content that meets the specifications of the Implementation Guides. This requires a number of changes in the software that produces or receives these transactions. Examples include new mappings in translators, new data edits, expanded data capture screens in source and billing, augmented billing systems, updates to adjudication systems, and all other systems that interface

with these transactions. In many cases, the problems found during transaction testing will need to be corrected in the business system rather than in the translator maps.

Once trading partners candidates have internally tested their HIPAA transaction compliance, they should consider using a third party to certify the trading partners as "compliant" with the HIPAA Implementation Guides. The timeframe for testing among trading partners could be dramatically reduced if each one is certified to meet the requirements of the HIPAA Implementation Guides, thereby assisting in the implementation of the transactions and code sets and reducing the cost of implementation. Considerable savings can be realized when an entity chooses to certify in lieu of the current trading partner- based method of testing.

Compliance testing is a process that applies to both outgoing as well as incoming transactions. While outgoing transactions are relatively easy to produce from actual data in a production system, incoming transactions present a particular problem. The traditional method to test incoming transactions has been to engage a trading partner that can produce relatively clean outgoing transactions. This, for HIPAA compliance, presents several unique problems. Some trading partners are not yet ready to produce outgoing transactions. If they can produce outgoing transactions, the test data could contain errors and thus be unsuitable to test incoming capabilities. Even in the best trading partner based test scenario, in order to fully test the ability to receive HIPAA transactions, the tests must include both compliant and non-compliant scenarios, making it very difficult to test using trading partner data. The use of structured test files with predictable errors becomes an absolute requirement. This sub workgroup has produced a substantial number of test files and is looking for additional volunteers to continue producing test files for all HIPAA transactions. These test files can be accessed via a link from the WEDI SNIP web page and downloaded for free. Please go to http://snip.wedi.org web page and follow the Other HIPAA Resources link located on the left side of the page, then click on the "Transaction Code Sets and Standards" link, followed lastly with the "WEDI SNIP EDI Test Files" link.

The business requirements of the HIPAA Implementation Guides are such that the testing of outgoing transactions is best performed with real production data rather than with synthetic test data. Using real production data for testing will uncover not only X12 format deficiencies, but also structural and data deficiencies in the production system, and may lead to corrections of issues previously identified during gap analyses.

Incoming test transactions, if they are to be taken to the adjudication or processing system, will need to contain real patient and provider data. For example, in order to test the claim status inquiry, the test data should represent previously filed claims as well as synthetic claims. Creating this sort of test data that covers all aspects of the transaction under test is not a trivial problem. Testing at this level with a cooperating trading partner will require a time consuming and expensive effort. Not testing the incoming transactions in this manner could result in substantial problems once the systems are put in production.

Given the need in most cases to test with real transaction data produced by a "live" system, it should be noted that any testing performed with a third party after April 14, 2003 is subject to the HIPAA Privacy requirements with respect to the confidentiality of patient identifiable information. All precautions should be taken to eliminate the possibility that patient information be exposed.

In spite of all the automated testing, and even having a third party certification of compliance, it will still be necessary to assure the integrity of the data when completing a "round trip." This white paper does not deal with the necessary testing of the application and adjudication systems. These systems must be tested to ensure that data elements are not truncated, ignored, or mis-processed in other ways (e.g., routing, use of a store and forward methodology). The testing of these applications is out of scope for this white paper. *(Refer to the WEDI SNIP Business-To-Business Transaction Testing White Paper for additional information on this topic.)*

This white paper focuses on the transaction compliance testing and certification of compliance, rather than the testing between trading partners. While references are made specifically to payers it should be

noted that those references are to particular transactions where the payer is the receiver of the transaction, such as the claims. There are other transactions where the receiver is not a payer and the roles are reversed.

Contrary to popular belief, no amount of testing or the certification of transactions for compliance can guarantee that all transactions generated by a specific trading partner will continually meet HIPAA requirements. While testing and certification should occur prior to putting a trading partner into production mode, compliance testing and third party certification should not eliminate the need for the receiver of the transaction to screen every one received in order to check for minimal compliance with the Implementation Guides. Changes to the standards can happen frequently, therefore the continual re-testing and possible re-certification of the production data stream are necessary elements of a HIPAA covered entity.

It is also imperative to point out that each covered entity is responsible for its own compliance with the HIPAA mandates. It is a misconception to believe that the vendors or clearinghouses related to a covered entity can bring that entity into HIPAA compliance. For example, if a provider uses a clearinghouse for the translation and routing of its transactions, the provider cannot assume that it is in compliance with the HIPAA mandates simply because the clearinghouse has proven the ability to generate a HIPAA-compliant transaction. The provider must look at its own ability to generate the data elements needed by the clearinghouse to translate that non-compliant data into a standard transaction. It also must begin to look at the code sets (both internal and external to the implementation guides) that it uses and make decisions as to whether to incorporate the standard code sets into its internal processes or to crosswalk its existing codes to the standard codes named in the implementation guides. This point is especially important for those entities that automatically post incoming transactions to any internal systems (e.g., a provider who systematically posts incoming 835s to an internal accounts receivable system). The provider must also work very closely with the technical staff of the clearinghouse to decide what values should be populated in the fields where the provider cannot provide the data elements from its internal processes to populate the required X12N fields. All of this must be accomplished in addition to ensuring compliance with the Security and Privacy rules when mandated by the HIPAA legislation. In summary, every entity covered under the HIPAA legislation needs to perform a detailed gap analysis of its processes and procedures to ensure that all areas of its operation have been reviewed and updated as necessary. Relying on a business associate for HIPAA compliance, even when the business associate has certified its own compliance, should never replace the covered entity's own due diligence.

Business Drivers

The reasons for writing this white paper are:

- To provide the health care industry with an outline of **issues** required to be addressed during the transaction testing and HIPAA transaction compliance certification process.
- To provide a level of **consistency** across the industry related to transaction testing methods and HIPAA transaction compliance.
- To attempt to **reduce administrative costs** of transaction testing by eliminating the repeated testing of the same basic functionality among each pair of trading partners
- To document the option of either taking advantage of third party certification or gaining HIPAA compliance via extensive trading partner testing.
- To provide for a mechanism by which a trading partner may **recognize** systems as compliant with the HIPAA transactions in an effort to expedite the testing process between all covered entities.

Because it is not the intention of WEDI SNIP to promote or advocate any product or service, this white paper documents the options that a covered entity has in its compliance efforts in regards to testing and possibly certifying its transactions. While this sub-workgroup supports the certification approach to compliance, it is noted that each covered entity needs to assess their choices and move forward with the approach that best fits the entity's needs and situation. Since there is not a current method of certifying the certification tool or service, creating an accrediting agency to certify the certifying tools/services may be the appropriate thing to do. However, the Department of Health and Human Services and the Center for Medicaid and Medicare Services have determined, since they are also a covered entity under the HIPAA regulations, that the role of certifying the certifier should not be theirs. As a result, the industry must determine what the best practices and processes are to determine the certification and testing products and tools they choose to utilize.

This group does recommend the formation of an industry consortium of those vendors who develop and support certification tools and services. Because there is not a certifier of the certification tools/services, the formation of this consortium could lead to uniform and consistent interpretation of the Implementation Guides, leading to a uniform implementation across all testing and certification tools and services. The Implementation Guides are sometimes vague in the requirements of each transaction. A consensus of industry vendors in a consortium would all but eliminate the expected disagreements in the interpretation of the intent of each guide.

There is no current mandate from federal oversight agencies that entities must be certified in the Transactions and Code Sets Rule. It is only a recommendation. It would be in the best interest of all covered entities to utilize the WEDI SNIP- recommended types of testing and to validate transactions before testing with each other. While there is merit in utilizing the test cases and testing methodology from a "certification" source, it should not be taken on faith that becoming certified relieves the trading partner from testing and validating EDI transactions. It is only suggested that doing so will allow the entity to significantly decrease testing time and dollars.

Background

Subtopic 1: What are the differences between transaction compliance testing and certification?

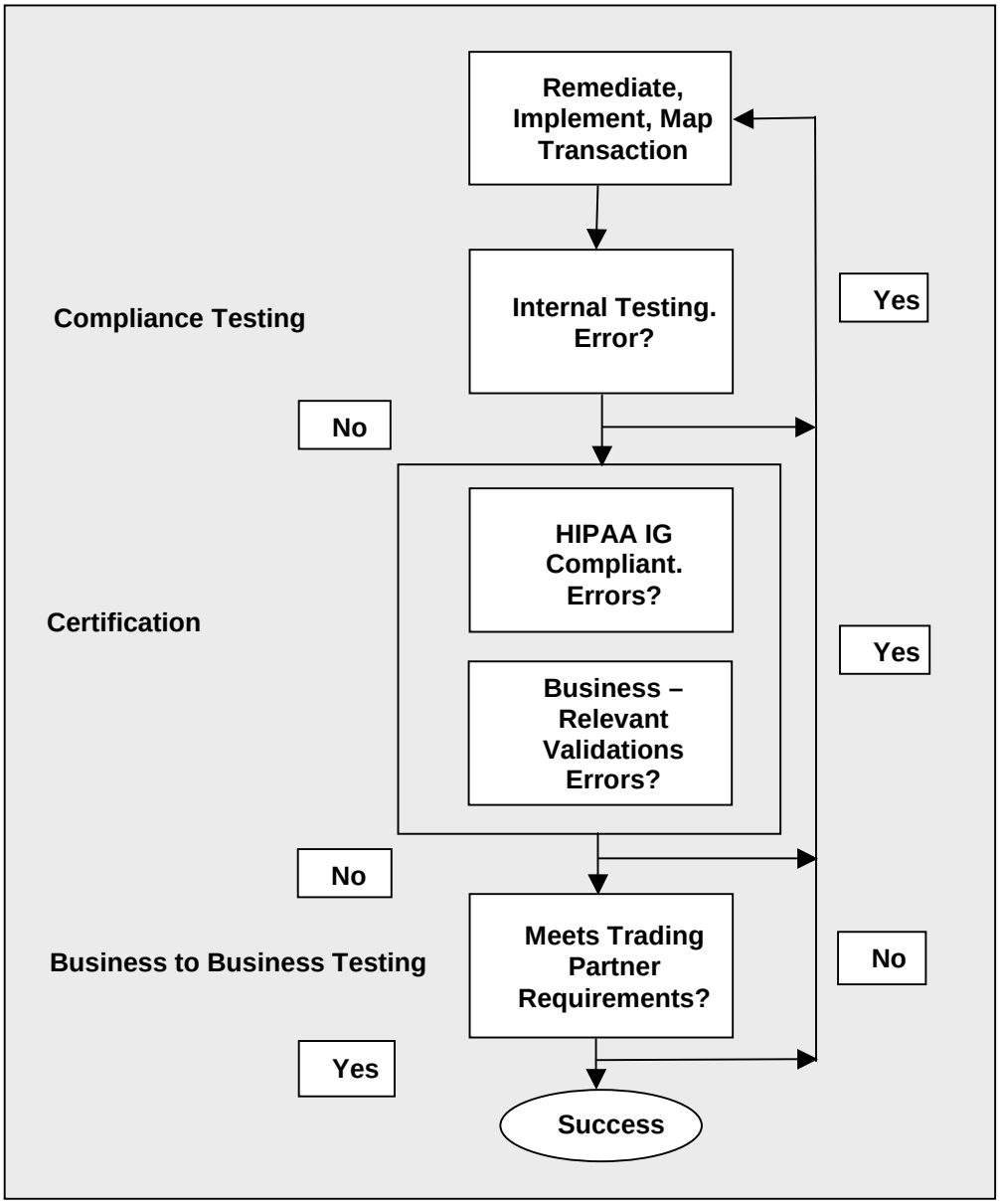
The concepts of testing, validation, verification, and certification seem to overlap to some extent and could benefit from clarification. Since this sub-workgroup has prepared two white papers on these topics, it becomes necessary to distinguish between these concepts as used in the white papers, in order to better determine the scope of each white paper and help in understanding the differences between these terms as used here.

We are using the term "testing" for two significantly different concepts. The first use of the term "testing" is for the type of testing done during the development of the EDI transactions by the HIPAA covered entity or its business associate. This EDI development needs to be tested in several ways before involving trading partners. We call this "compliance testing". The testing may include: unit testing, module testing, and regression testing, and culminate in compliance certification. It is necessary to conduct this testing before any trading partners are involved, to have some sense of the degree of compliance. This testing could be conducted between two cooperating trading partners, but it is best conducted with special purpose EDI tools such as HIPAA specific test transaction suites, syntax validation tools, and HIPAA specific compliance test tools. Some translator packages provide these sorts of HIPAA EDI toolkits, and the products and services listed in the Vendor Listing also provide assistance with this testing. This is the testing concept addressed by this white paper. We call this testing "transaction compliance".

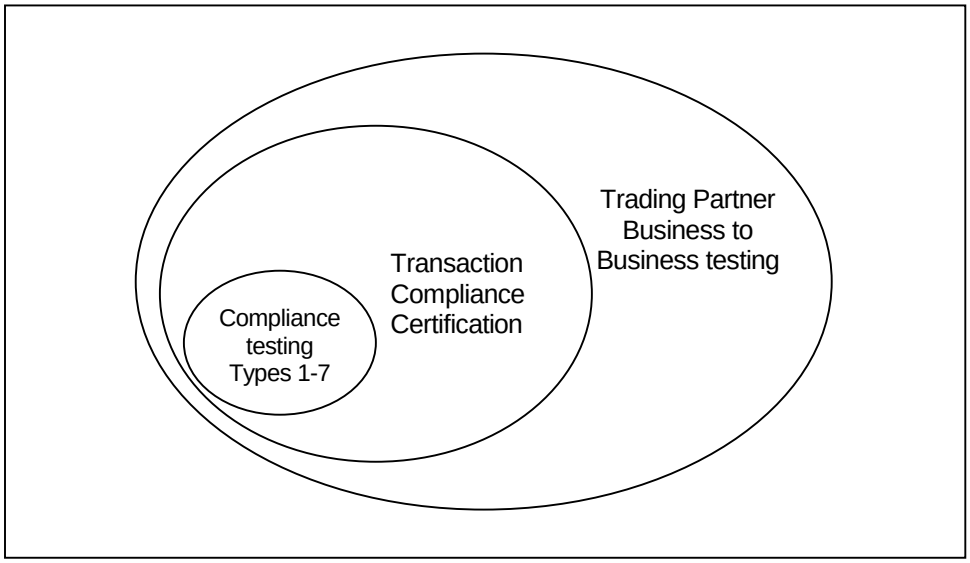
The second use of the term “testing” extends beyond the scope of EDI testing, into the interoperability testing between two trading partners. This covers issues such as telecommunications connectivity, security, data integrity, round-trip integrity, stress testing, etc. This type of testing, by its nature, must be performed between two trading partners. This is the testing described in the WEDI SNIP “Business-to-Business Testing White Paper”.

Since Transaction Compliance has traditionally been done as part of the establishment of each new trading partner relationship, it is traditionally conducted as part of the business-to-business testing, and not as a separate task. The consequence of this is that the transaction compliance is repeated each time a new trading partner relationship is established. If the trading partners were to segregate the transaction compliance task in such a way that it does not need to be repeated for each trading partner, the savings accrued would be substantial.

While compliance testing can easily detect the non-compliant situations and errors, the determination that an EDI transaction is error free does not necessarily imply that it is compliant with the Implementation Guide. The Implementation Guides have a minimal set of requirements that must, by their nature, apply to all transaction variants. In order for a transaction to be truly in compliance with the Implementation Guide, it first must pass these common minimal requirements, and then also pass the business requirements of the Implementation Guide as it applies to the covered entities and the type of transaction. For instance, an ambulance claim without miles, or an anesthesia claim without minutes could very well be error free, but incomplete. This is a critical difference between a transaction that is error free and one that is certifiable as HIPAA compliant.



Certification plays a role in between the two types of testing described above. Upon the successful completion of compliance testing, the individual entity should go through a third party evaluation of the transaction compliance. Since not every trading partner must implement all the possible functionality of each one of the HIPAA transactions, especially concerning different product types or line of services, it is important that the certification be specific to the functionality that pertains to the business of the individual entity. Otherwise the certification process could result in certifying transactions that are compliant with the Implementation Guide requirements but are not relevant to the business of the entity(such as certifying the HIPAA compliance of an ambulance provider based on the submission of office visits).



This white paper explores the compliance testing requirements and the characteristics of Certification for HIPAA EDI compliance. The goal is that these certifications should reduce or eliminate the need to repeat the Transaction Compliance testing between each pair of trading partners, and the Certified trading partners can possibly go directly into business-to-business testing based on trading partner preference.

Subtopic 2: What are the different types of testing necessary for HIPAA transaction compliance?

Different transaction certification systems will conduct different types of testing. This testing will vary from a basic syntactical integrity checking to a more intricate situational testing. It is the purpose of this subtopic to define those different types of testing that should be considered to assess HIPAA compliance of a transaction.

The recommended types of testing are all necessary for compliance with HIPAA. Under HIPAA, the Secretary has adopted a series of standards. Some of these standards are represented by X12 and NCPDP syntactical requirements. Other standards are represented by the business rules and situational requirements in the Implementation Guides. Yet, other standards adopted under HIPAA are not in the Implementation Guides, but in code sets, or the coding guidelines that are incorporated into these code sets. In order to be deemed HIPAA compliant, the transactions must be compliant with **all** of those requirements, not just with a selected few.

However, even though all types of testing are necessary for HIPAA compliance, the trading partner candidate may choose to conduct certain tests with the assistance of testing software or a testing service, and other tests with the assistance of cooperating trading partners.

The types of testing for HIPAA transaction compliance are applicable both to outgoing as well as incoming transactions.

Subtopic 3: What types of transaction testing are recommended as the minimal necessary before starting "business-to-business" testing between providers and payers. In addition, what types of testing are recommended as acceptable for an entity's approval processes?

At a minimum, all trading partners should test for syntactical compliance with the HIPAA requirements of the transactions by themselves, prior to testing with outside trading partners. Not doing so may impose their internal testing needs against another trading partner, therefore decreasing the goal of minimal basic EDI testing between partners. If a covered entity has performed all of the recommended types of testing outlined below and obtained third party certification, trading partners may be able to accept the validity of the HIPAA transaction compliance established by the third party certifier to reduce testing through their own systems.

If a covered entity has only performed several of the types of testing, but not all, they should be expected to test with each trading partner for at least all the types of testing that were not tested during the compliance process. Given that some of these test types are interrelated, it is possible that the transaction compliance, when done by a trading partner, may necessitate repeating some of the test types multiple times.

The objective of certification is that a certified covered entity not be required to repeat the transaction compliance testing with each and every one of their trading partners. This will create quicker business- to -business testing turnaround timeframes and expedite the implementation of the HIPAA transaction sets.

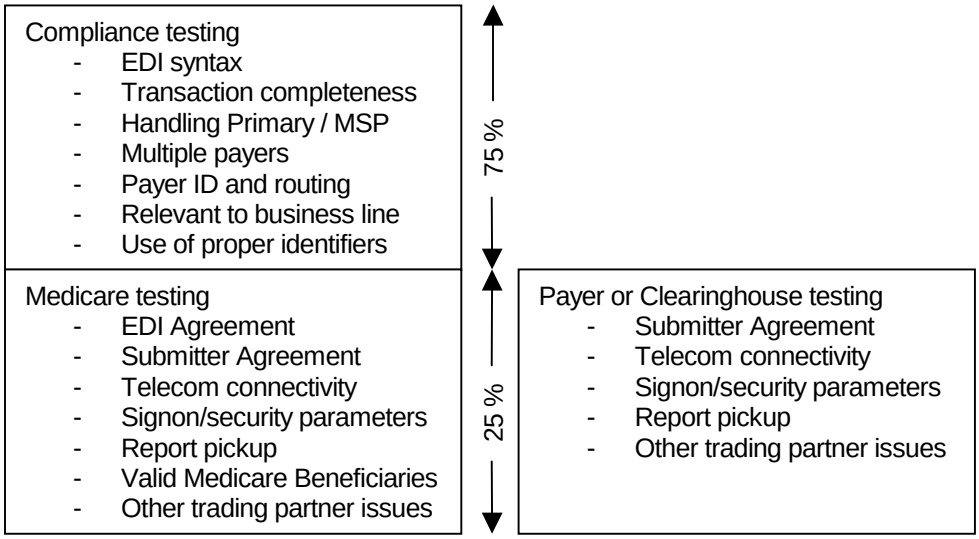
Traditionally, large payers and clearinghouses have conducted most of the testing of healthcare EDI transactions. In this environment, the entire test suite has been customized to fit the needs of the payer or clearinghouse conducting the testing, as shown in the diagram below.

Medicare Carrier or Intermediary
- EDI Agreement
- Submitter Agreement
- Telecom connectivity
- Signon/security parameters
- EDI syntax
- Transaction completeness
- Handling Primary / MSP
- Report pickup
- Relevant to business line
- Use of proper identifiers
- Valid Medicare Beneficiaries
- Other trading partner issues

Payer or Clearinghouse
- Submitter agreement
- Telecom connectivity
- Signon/security parameters
- EDI syntax
- Transaction completeness
- Multiple payers
- Payer ID and routing
- Report pickup
- Use of proper identifiers
- Other trading partner issues

Today, the testing activities of the different payers and clearinghouses have much in common but they are not structured in a way that the industry could take advantage of the commonality. Each provider is tested from scratch every time. The fact that a provider is sending production claims to Medicare, in general, does not reduce the time it takes to test this provider with Medicaid or a clearinghouse. Ideally, the industry should be able to take advantage of these efficiencies. This is one of the goals of the white papers developed by the Testing Sub-workgroup.

Under HIPAA, the importance of the common aspects of testing is magnified by the depth and breadth of the Implementation Guide requirements. Compliance testing of the HIPAA transactions takes more than 75% of the effort, even with experienced trading partners. This commonality approach lends itself to untapped savings. For example, if we organize the testing by separating the process into "compliance testing" versus "business-to-business testing" we could obtain a result like the following figure.



In this case, the compliance testing is performed only once and does not need to be repeated for each trading partner. The savings accrue for both the provider and the payer or clearinghouse. If, under HIPAA, the compliance testing takes 75% of the test

time, a provider with four trading partners (typical case where the provider has a direct connection to Medicare, Medicaid, the local Blue Plan, and a clearinghouse) will see a reduction of its testing effort from 1+1+1+1=4 to 0.75+0.25+0.25+0.25+0.25=1.75. And each one of the payers or clearinghouses will see a reduction of their testing effort to one fourth. For this to happen, the compliance testing must be independent of any one trading partner, and acceptable to multiple trading partners without having to repeat it.

Even in cases where the covered entity only establishes one trading partner relationship, such as designating a clearinghouse through which all transactions flow, there is no additional cost, as the Transaction Compliance Testing must also be conducted in those instances. If the transaction compliance testing is acceptable to multiple trading partners, the establishment of all subsequent trading partners benefits from savings of about 75% of the implementation effort.

Subtopic 4: What other issues, related to transaction testing, should be considered for successful compliance testing, certification and payer acceptance?

A covered entity should consider a third party certification mechanism for the integrity of the data when translated by a clearinghouse. Even though a clearinghouse or software package may have tested and certified the ability to correctly produce HIPAA compliant transactions and correctly receive compliant transactions, there are many other sources of error or missing data that are outside of the control of the software or clearinghouse. This is especially true when translating from/to a variety of pre-HIPAA legacy formats such as the NSF, UB92, or other proprietary formats. In these circumstances, the potential for missing data, data corruption, or truncation is very real. Most legacy transactions do not have detailed business rules as the HIPAA transactions do. In most cases they do not go beyond the format specifications for the trading partner that owns that version of the specifications. We suggest a mechanism to certify data integrity for a trading partner when sending transactions through a clearinghouse, otherwise each pair of trading partners would have to do their own independent verification of the “pass through” integrity of the data going through a clearinghouse.

Protection of patient information should be carefully maintained when testing the HIPAA transactions. Testing these transactions requires the use of live data in order to have results that truly represent the actual covered entity business scenarios. Testing with synthetic transactions, although useful in the syntax compliance phase, does not accurately represent the business needs unless the synthetic test transactions are carefully crafted for each pair of trading partners. This could potentially produce a gap in the process and ultimately reduce the trading partner acceptance rate of certain certification systems. Therefore, it becomes imperative that certification be done on real production transactions, and thus use Protected Health Information that must be secured.

Testing should not be limited to the April-October 2003 timeframe required as a minimum by the Administrative Simplification Compliance Act (ASCA). It is strongly recommended that Compliance testing and certification be started as soon as possible, and definitely well before April 2003. It is also recommended that trading partner testing begin as soon as possible on a limited basis, to allow time for identification and resolution of differences between compliance and certification tools within trading partner communities.

Subtopic 5: What entities provide testing facilities today? What types of transaction compliance testing do they provide? Do they provide certification?

A listing of the companies offering transaction compliance testing and certification services/products discovered by this sub-workgroup to date can be found in the Vendor Listing on the WEDI SNIP web site at http://snip.wedi.org.

The table of information about testing and certification software and services in the Vendor Listing is for reference use only and only reflects those vendors who offer software packages and services that this sub workgroup has identified. This sub workgroup presents information that its members are aware of, and was obtained without conducting surveys. No formal or informal evaluations were performed in order to create information presented in the Vendor Listing nor does the listing of an organization in the listing imply any sort of endorsement by the sub workgroup.

Subtopic 6: Who will certify the Certification Services?

Given that the bulk of testing may reside with these Certification tools/services, what are the assurances that the certifier is correctly testing for any particular trading partner?

In the Transactions Final Rule this topic received some attention. Given that the Department of Health and Human Services (HHS) and the Center for Medicare and Medicaid Services (CMS) are themselves covered entities, it would not be appropriate for either to act as the certification service or even in the role of "certifying the certifier" as this could constitute a conflict of interest.

It has been left to the industry to determine which certification services are deemed appropriate. This sub workgroup encourages the use of a transaction compliance testing product or service that is most appropriate for each trading partner. There are two approaches to qualify a Certification tool/service as a valid choice for industry constituents:

A) Accredit the HIPAA Transaction Compliance Certification Services through a neutral accreditation program built specifically for the accreditation of such Services. The accreditation program could build the criteria necessary to certify that a particular Compliance Certification Service has met or exceeded the criteria built by the accrediting organization.

B) Trading partner community acceptance of any particular transaction compliance certification tool/service that acts as ratification that the Certification Service is performing as needed to benefit the industry.

Today, payers require some level of transaction compliance testing to occur between themselves and the providers before allowing the providers to send production transactions. With a Compliance Certification tool/service that provides adequate compliance testing functionality for the payer, the payer may choose to allow submitters who are certified to send production transactions without providing for additional transaction compliance testing at the payer site. This same statement applies to providers who will be receiving the 835 and other transactions.

Subtopic 7: What do we recommend in selecting a compliance testing system or service?

How will payers, providers, clearinghouses and vendors choose the right compliance testing Service?

Today, payers conduct limited compliance tests as part of the testing with each trading partner and before allowing the submitter to send production transactions. Each payer's test system provides the focused functionality necessary to assure that payer that once any particular submitter has passed transactions successfully through the test system, future transactions coming from that submitter will be relatively error-free. The submitter is then approved to submit production transactions.

Now, with the HIPAA legislation going into effect, covered entities are tasked with ensuring that their transactions are HIPAA-compliant before beginning their trading partner testing. Several tools are available to assist in this testing process (some of these tools are listed in the Vendor Listing. Information on translation tools is available in the Translator White Paper available on the WEDI SNIP web site). These tools will assist the entity in their HIPAA compliance and most likely expedite the implementation.

If an entity desires to evaluate a testing or certification tool or service, here is an example of how the evaluation process might work:

Using the claim as the example transaction, with the provider as the sender of the transaction and the payer as the receiver, we could describe a sample process as follows:

1. The payer evaluates their current compliance test system as a reference point to set the requirements for acceptance of the provider's claims. By performing this evaluation the payer knows what minimal testing the Certification tool/service will need to provide in lieu of the payer's own compliance testing method.

2. The payer selects some providers to conduct an assessment of the compliance testing with the Certification tool/service, or the payer may choose to send their own test files through the Certification tool/service to validate the testing processes. The payer will want to test the same files through the payer's own test system to validate that the results are similar. A variety of test scenarios and business cases may have to be processed in this manner before the payer approves the Certification tool/service in lieu of, or in addition to, the payer's own compliance testing.

3. Once the Certification tool/service has been approved, it will not change the method used for certification without the payer's knowledge. This will assure the certification results remain consistent between all submitters.

4. The payer will then accept the provider's transactions from certified providers without requiring further compliance certification. If a provider has not been certified, the payer will have to conduct the compliance testing of that provider as one of the preliminary steps in the business-to-business testing.

   In certain cases, such as providers choosing compliance testing and a certification service to use, the choice will simply be determined by the scope and number of the payers that accept the certification service in lieu of repeated testing.

Because of the lack of standardization of the criteria for testing and certification, we are recommending the formation of a consortium of those vendors who supply testing and certification tools. The formation of this consortium will help to ensure the consistent interpretation of the Implementation Guide rules and the consistent rollout of those rules as they are incorporated into the various tools/services.

Recommendation for Solution

Subtopic 1: What are the differences between transaction compliance testing and certification?

As described in the background section, there are significant differences between compliance testing and certification. Each trading partner candidate has several options for compliance testing. The current practice is that the Transaction Compliance testing is included as one of the steps of the Business-to-Business testing. This causes increased cost and complexity, by repeating the Transaction Compliance testing between each pair of trading partners. Separating the Transaction Compliance testing from the Business-to-Business testing, and the use of Certification to reduce or eliminate the need for repeated Transaction Compliance testing is a better alternative.

Recommendation: All trading partner candidates should go through Transaction Compliance testing before engaging into test transactions with trading partners. This compliance testing should be conducted with automated testing tools.

Recommendation: Trading partners should use third party transaction certification in order to reduce or eliminate the necessity of repeated transaction compliance testing. Trading partners should use/accept Transaction Certification by an acceptable third party in lieu of repeated Transaction Compliance Testing.

Recommendation: Transaction certification should be driven by the lines of business of each covered entity. These certified capabilities should be disclosed to trading partners and trading partner candidates.

Subtopic 2: What are the different types of testing necessary for HIPAA transaction compliance?

Assumptions: It is assumed that the types of testing are somewhat independent of each other. If a compliance certification system performs different types of testing, it will be noted as such within their information. However, types 1 and 2 are pre-requisites for the other types of testing.

In the past this white paper had referred to these types of testing as "levels". However, the word "level" gave the incorrect impression that these types of testing built on each other in some manner, and that the testing could be stopped at a certain level. In order to try to correct this misperception, we are now calling them "types" of testing, more clearly conveying the notion that they are independent of each other. We recommend that all of these types of testing be completed for HIPAA compliance.

Recommended Types of Testing:

Type 1: *EDI syntax integrity testing* – Testing of the EDI file for valid segments, segment order, element attributes, testing for numeric values in numeric data elements, validation of X12 or NCPDP syntax, and compliance with X12 and NCPDP rules. This will validate the basic syntactical integrity of the EDI submission.

Type 2: *HIPAA syntactical requirement testing* – Testing for HIPAA Implementation Guide-specific syntax requirements, such as limits on repeat counts, used and not used qualifiers, codes, elements and segments. Also included in this type is testing for HIPAA required or intra-segment situational data elements, testing for non-medical code sets as laid out in the Implementation Guide, and values and codes noted in the Implementation Guide via an X12 code list or table.

Type 3: *Balancing* – Testing the transaction for balanced field totals, financial balancing of claims or remittance advice, and balancing of summary fields, if appropriate. An example of this includes items such as all claim line item amounts equal the total claim amount. (See pages 19-22, *Healthcare Claim Payment/Advice – 835 Implementation Guide for balancing requirements of the 835 transaction*.)

Type 4: *Situation testing* – The testing of specific inter-segment situations described in the HIPAA Implementation Guides, such that: If A occurs then B must be populated. This is considered to include the validation of situational fields given values or situations present elsewhere in the file. Example: if the claim is for an accident, the accident date must be present.

Type 5: *External code set testing* – Testing for valid Implementation Guide-specific code set values and other code sets adopted as HIPAA standards. This level of testing will not only validate the code sets but also make sure the usage is appropriate for any particular transaction and appropriate with the coding guidelines that apply to the specific code set. Validates external code sets and tables such as CPT, ICD9, CDT, NDC, status codes, adjustment reason codes, and their appropriate use for the transaction.

Type 6: *Product types or line of services:* This testing type is required to ensure that the segments/records of data that differ based on certain healthcare services are properly created and processed into claims data formats. These specific requirements are described in the Implementation Guides for the different product types or lines of service. For example, ambulance, chiropractic, podiatry, home health, parenteral and enteral nutrition, durable medical equipment, psychiatry, and other specialized services have specific requirements in the Implementation Guide that must be tested before putting the transaction in production. This type of testing only applies to a trading partner candidate that conducts transactions for the specific line of business or product type.

Type 7: Implementation Guide-Specific *Trading Partners:* The Implementation Guides contain some HIPAA requirements that are specific to Medicare, Medicaid, and Indian Health. Compliance or testing with these payer specific requirements is not required from all trading partners. If the trading partner candidate intends to exchange transactions with one of these Implementation Guide special payers, this type of testing is required. When a certification service certifies a trading partner for compliance, the certification service must indicate whether these payer specific requirements were met during the certification process. Other payers and trading partners may have their own specific business requirements; but, unless they are listed in the HIPAA Implementation Guides, they are not HIPAA requirements. These non-HIPAA trading partner specific requirements must be tested as part of the business-to-business testing. For further information on business-to-business testing and for further information on testing trading partner rules that are not contained in the Implementation Guides, please see the Business-To-Business Testing White Paper developed by this sub-workgroup.

Subtopic 3: What types of transaction testing are recommended as the minimal necessary before starting "business-to-business" testing between providers and payers. In addition, what types of testing are recommended as acceptable for the entity's approval processes?

It is possible that standards be established for the testing process between providers, clearinghouses, and payers such that the use of compliance testing and transaction certification becomes customary before starting the business-to-business testing and results in the reduced testing time among the trading partner systems. Ideally, a provider that has successfully completed compliance testing and/or has been certified to be in compliance with the HIPAA Implementation Guides would be ready to begin trading partner testing. The same would apply to the payers or the transactions they generate.

Therefore a trading partner who has completed testing on all six (or seven if appropriate) types of testing mentioned in Subtopic 2, would have no compliance testing required at all with any of the trading partners they would submit to. A submitter who has been tested only, for example, for types 1, 2, and 3 tests, would have to test for the other types with each one of its trading partners.

Recommendation: All trading partners must test their transactions for types 1 and 2 at a minimum before attempting to exchange test data with another trading partner. A transaction that does not meet the syntactical requirements of a HIPAA transaction should not be transmitted, even as a test, to a trading partner.

Recommendation: In order to reduce the testing costs and to expedite the implementation process, trading partners should test their transactions for all the relevant types of testing described above with compliance testing software and a third party compliance testing tool/service.

Recommendation: The receiving trading partners should consider accepting transactions from a submitter that has completed testing or has been certified to comply with types 1 through 6 (or 7 if one of the trading partners is a trading partner that has specific Implementation Guide requirements) for the kinds of business content reflecting the trading partner's business, without requiring any further compliance testing.

Recommendation: In order to reduce the overall testing costs and to expedite the implementation process, "receiving" trading partners should test their translators and their maps for incoming transactions with data sufficient to represent the possible transactions received. This testing should not be dependent on finding trading partners willing to send the relevant transactions, but should be established **before** the receiving system starts testing with trading partners or goes into production.

Subtopic 4: What other issues, related to transaction testing, should be considered for successful compliance testing, certification, and payer acceptance?

Recommendation: Covered entities should not rely on the certification of their business associates, vendors, or clearinghouses as sufficient for their own HIPAA compliance. It is up to each covered entity to perform its own gap analysis and

transaction and code sets determination of compliance. Simple reliance on a business associate, vendor, or clearinghouse determination of compliance is no substitute for due diligence.

Recommendation: Whenever possible, patient Identifiable Information should be suppressed or converted into non-identifiable information from tests submitted to third parties, either as part of compliance testing or business-to-business testing. If the testing systems receive patient identifiable information, the testing systems must be in compliance with the HIPAA regulations concerning security, privacy, and business associate agreements.

Subtopic 5: What entities provide testing facilities today? What types of transaction compliance testing do they provide? Do they provide certification?

Recommendation: The Vendor Listing contains a listing of some of the certification and testing systems and services available on the market today. It is not the intention of this white paper to promote any particular system or service mentioned below. These are merely examples of systems and services available and this list is not inclusive of all testing systems and services, simply a sample of what is in the market today. The information represented in the Vendor Listing has been provided by the listed entities themselves and has not been verified by this Sub Workgroup.

Subtopic 6: Who will certify the Certification Services?

It has been left up to the industry to determine which certification services are deemed appropriate. This sub workgroup encourages the use of the transaction compliance testing product or service that is most appropriate to each trading partner.

Recommendation: Accredit the Transaction Compliance Certification Tools/Services through a neutral accreditation program built specifically for the accreditation of HIPAA Compliance Certification Tools/Services. The accreditation program should build the criteria necessary to certify that a particular Certification Tool/Service has met or exceeded the criteria built by the accrediting organization.

Recommendation: Form a consortium of vendors who offer Certification Tools/Services to ensure the uniform translation and implementation of Implementation Guide rules. This consortium could work in conjunction with X12N and NCPDP to identify and resolve guide inconsistencies and incorporate these decisions into the tools.

Subtopic 7: What do we recommend in selecting a compliance testing system or service?

Recommendation: In selecting a compliance testing system or service, payers and providers should conduct a methodical comparison of the results obtained by the payer's/provider's own compliance testing and the results provided by the compliance testing system/service.

Value in Accepting

The value in accepting the recommendations of this white paper accrues immediately to all HIPAA covered entities. If instead of repeating the Transaction Compliance Testing with each trading partner as part of the establishment of the trading partner relationship, the HIPAA covered entities conduct Transaction Compliance independent of their trading partners and before establishing the trading partner relationship, the effort spent in establishing each trading partner relationship may be reduced to about 25% of the current industry effort, and the savings are reflected both in direct costs and time spent by both trading partners.

The Vendor Listing contains a table of organizations offering transaction compliance testing and certification services. The value in accepting the preceding recommendations, testing for compliance, and becoming certified through an organization like the ones on the Vendor Listing table, will be to provide guidance to health plans, health care providers, and clearinghouses regarding the testing process.

By following these recommendations and becoming Certified, the testing timeframes with Business Partners and Associates will undoubtedly be drastically reduced, resulting in the implementation of the HIPAA standard transactions in a timely fashion and at a much lower cost.

Acknowledgments

The WEDI SNIP Transaction Set Testing Sub Workgroup is comprised of organizations from all facets of the Health Care Industry. The following list represents many of the organizations participating in this Testing Sub Workgroup. The members of these organizations have volunteered their time and energies and are greatly appreciated and acknowledged.

Advent Software, Ltd.
AXIOM Systems
Blue Cross Blue Shield of Florida
Blue Cross Blue Shield of Kansas
California Association of Health Plans
California Department of Health Services
Center for Medicare and Medicaid Services
CIGNA
Claredi - special thanks to Kepa Zubeldia, co-author of this document
The Cleveland Clinic
Covansys, Inc.
Edifecs, Inc.
Electronic Data Systems (EDS)
Empire Blue Cross Blue Shield – special thanks to Suzan Ryder, Testing SWG Co-Chair
Foresight Corporation
Gartner Group
GE Global Exchange Services, Inc.
HDX
IDX
IHC
John Muir / Mt Diablo Health System
Mayo Clinic
McKesson HBOC - special thanks to Mark McLaughlin, co-author of this document
Missouri Medicaid
Proxy Med

State Farm Insurance Companies
Strategic Systems Solutions, LLC
Sybase
Verizon Information Technologies, Inc. – special thanks to John Lilleston, Testing SWG Co-Chair and White Paper Facilitator
Washington Department of Health Services